

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250571

(43)Date of publication of application : 17.09.1999

(51)Int.Cl.

G11B 20/10
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : 10-052423

(22)Date of filing : 04.03.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

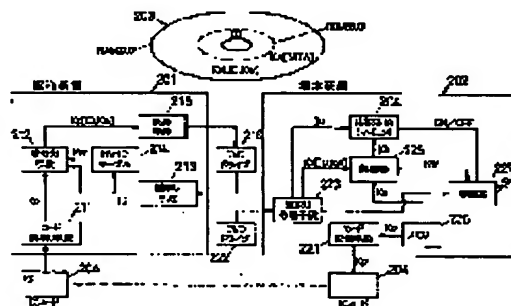
(72)Inventor : TAKECHI HIDEAKI
GOTO SHOICHI
IIZUKA HIROYUKI
YAMADA MASAZUMI

(54) INFORMATION DISTRIBUTING DEVICE, TERMINAL DEVICE AND INFORMATION DISTRIBUTING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information distributing device, terminal device, and an information distributing system by which unauthorized copy to an other recording medium and use without permission can surely be prevented.

SOLUTION: A distributing device 201 is constituted with a card reading means 211 reading information of an IC card 204, a reading means 213 reading information of a DVD-RAM, a recording means 215 recording information in the DVD-RAM, a Kw ID table 214 converting an ID number to a cipher key Kw, and a ciphering means 212 ciphering information, and a terminal device 20 is constituted with a card recording means 221 recording information in the IC card 204, a memory 226 having a public key Kp and a secret key Ks, a reading and separating means 223 reading information of the DVD-RAM and separating it, decipherers 225, 227, deciphering ciphered information, and a comparing means 224 comparing two IDs.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51) Int.Cl.⁶

識別記号

F I

G 1 1 B 20/10

G 0 6 F 12/14

G 0 9 C 1/00

H 0 4 L 9/32

3 2 0

6 3 0

G 1 1 B 20/10

G 0 6 F 12/14

G 0 9 C 1/00

H 0 4 L 9/00

H

3 2 0 E

6 3 0 F

6 7 3 E

6 7 5 A

審査請求 未請求 請求項の数25 O L (全 12 頁)

(21) 出願番号

特願平10-52423

(22) 出願日

平成10年(1998) 3月4日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 武知 秀明

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 後藤 昌一

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 松田 正道

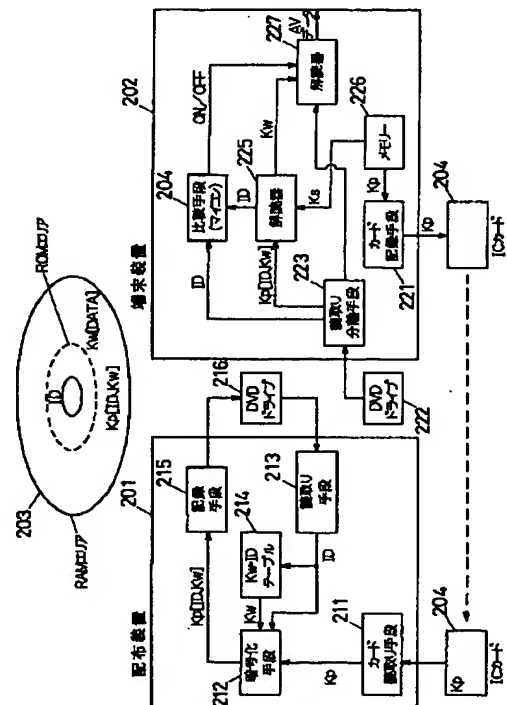
最終頁に続く

(54) 【発明の名称】 情報配布装置と端末装置及び情報配布システム

(57) 【要約】

【課題】 情報の配布に際し、鍵が盗まれたり、不正コピーが発生する恐れがあり、不正使用や無断使用を防止できない。

【解決手段】 配布装置201は、ICカード204の情報を読み取るカード読取り手段211、DVD-RAMの情報を読み取る読取り手段213、DVD-RAMに情報を記録する記録手段215、ID番号を暗号鍵Kwに変換するKw・IDテーブル214、情報を暗号化する暗号化手段212で構成され、端末装置202は、ICカード204に情報を記録するカード記録手段221、公開鍵Kpと秘密鍵Ksを持つメモリ226、DVD-RAMの情報を読み取り分離する読取り分離手段223、暗号化情報を解読する解読器225、227、2つのIDを比較する比較手段224により構成される。



【特許請求の範囲】

【請求項1】 記録媒体固有のID番号を持ち公開鍵K_pが記録された情報記録媒体から、前記ID番号及び公開鍵K_pを読み取る鍵読取り手段と、その読み取ったID番号及び所定の情報を前記読み取った公開鍵K_pにより暗号化する暗号化手段と、その暗号化したID番号及び所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項2】 請求項1の前記情報配布装置で、前記公開鍵K_pにより暗号化したID番号及び所定の情報が記録された前記情報記録媒体から、前記ID番号、暗号化ID番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記読み取った暗号化ID番号及び所定の情報を復号する復号化手段と、その復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項3】 請求項1の前記情報配布装置と、請求項2の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項4】 記録媒体固有のID番号を持つ情報記録媒体から、前記ID番号を読み取るID読取り手段と、公開鍵K_pが記録された鍵記録媒体から前記公開鍵K_pを読み取る鍵読取り手段と、その読み取った公開鍵K_pにより前記読み取ったID番号及び所定の情報を暗号化する暗号化手段と、その暗号化したID番号及び所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項5】 請求項4の前記情報配布装置で、前記公開鍵K_pにより暗号化したID番号及び所定の情報が記録された前記情報記録媒体から、前記ID番号、暗号化ID番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記読み取った暗号化ID番号及び所定の情報を復号する鍵復号化手段と、その復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項6】 請求項4の前記情報配布装置と、請求項5の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項7】 記録しようとするデータの識別情報が記録された情報記録媒体から前記識別情報を読み取る識別情報読取り手段と、その識別情報に基づいて所定の情報を生成する情報生成手段と、記録媒体固有のID番号及び公開鍵K_pが記録された鍵記録媒体から、前記ID番号及び前記公開鍵K_pを読み取る鍵読取り手段と、その

読み取った公開鍵K_pにより前記読み取ったID番号及び前記所定の情報を暗号化する暗号化手段と、その暗号化したID番号及び所定の情報と前記読み取った識別情報とを前記鍵記録媒体に記録する情報記録手段とを備えたことを特徴とする情報配布装置。

【請求項8】 請求項7の前記情報配布装置で、前記公開鍵K_pにより暗号化したID番号及び所定の情報と前記識別情報とが記録された前記鍵記録媒体から、前記ID番号、暗号化ID番号、暗号化された所定の情報及び、識別情報を読み取る暗号読取り手段と、前記識別情報に対応する暗号化ID番号及び所定の情報を選択する選択手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記選択した暗号化ID番号及び所定の情報を復号する復号化手段と、その復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、前記識別情報に応じて、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項9】 請求項7の前記情報配布装置と、請求項8の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項10】 記録媒体固有のID番号を持つ情報記録媒体から、前記ID番号を読み取るID読取り手段と、公開鍵K_pが記録された鍵記録媒体から前記公開鍵K_pを読み取る鍵読取り手段と、その読み取った公開鍵K_pにより前記読み取ったID番号及び所定の情報を暗号化する鍵暗号化手段と、その暗号化したID番号及び所定の情報を前記鍵記録媒体とは別の鍵記録媒体に記録する鍵記録手段とを備えたことを特徴とする情報配布装置。

【請求項11】 前記別の鍵記録媒体が、前記情報記録媒体の所定場所に設けられていることを特徴とする請求項10に記載の情報配布装置。

【請求項12】 請求項10または11の前記情報配布装置で、前記公開鍵K_pにより暗号化したID番号及び所定の情報が記録された前記別の鍵記録媒体から、前記暗号化ID番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記情報記録媒体からID番号を読み取るID読取り手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記読み取った暗号化ID番号及び所定の情報を復号する復号化手段と、その復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項13】 請求項10または11の前記情報配布装置と、請求項12の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項14】 記録媒体固有のID番号を持つ情報記録媒体から前記ID番号を読み取るID読取り手段と、

公開鍵K_pが記録された鍵記録媒体から前記公開鍵K_pを読み取る鍵読取り手段と、前記読み取ったID番号に基づいて暗号鍵K_wを生成する情報生成手段と、前記公開鍵K_pにより前記ID番号及び前記暗号鍵K_wを暗号化する暗号化手段と、その暗号化したID番号及び暗号鍵K_wを前記情報記録媒体に記録する情報記録手段とを備え、前記情報記録媒体に記録されるデータは暗号鍵K_aにより暗号化され、前記暗号鍵K_aは前記暗号鍵K_wで暗号化されて前記情報記録媒体に記録されていることを特徴とする情報配布装置。

【請求項15】 請求項14の前記情報配布装置で、前記公開鍵K_pにより暗号化したID番号及び暗号鍵K_wと前記暗号鍵K_wにより暗号化した暗号鍵K_aとその暗号鍵K_aにより暗号化したデータとが記録された前記情報記録媒体から、前記ID番号、暗号化ID番号、暗号化暗号鍵K_w及び、暗号化暗号鍵K_aを読み取る暗号鍵読取り手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記読み取った暗号化ID番号及び暗号化暗号鍵K_wを復号する鍵復号化手段と、その復号した暗号鍵K_wにより前記暗号鍵K_aを復号する暗号鍵復号手段と、前記復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、前記復号した暗号鍵K_aにより前記情報記録媒体に記録された暗号化データを復号するデータ復号手段とを備えたことを特徴とする端末装置。

【請求項16】 請求項14の前記情報配布装置と、請求項15の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項17】 前記情報記録媒体に記録された暗号化データは、複数個に分割されたものであって、その分割されたデータ毎に前記暗号鍵K_aが異なることを特徴とする請求項16記載の情報配布システム。

【請求項18】 記録媒体固有の暗号鍵KIDを持つ情報記録媒体から、前記暗号鍵KIDを読み取る読取り手段と、公開鍵K_pが記録された鍵記録媒体から前記公開鍵K_pを読み取る鍵読取り手段と、前記読み取った暗号鍵KIDにより所定の情報を暗号化し、更にその暗号化した所定の情報を公開鍵K_pにより暗号化する暗号化手段と、その暗号化した所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項19】 請求項18の前記情報配布装置で、前記暗号化した所定の情報が記録された前記情報記録媒体から、前記暗号鍵KID及び暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵K_pに対応する秘密鍵K_sを用いて、前記読み取った暗号化された所定の情報を復号し、更にその復号した所定の情報を前記暗号鍵KIDにより復号する鍵復号化手段とを備えたことを特徴とする端末装置。

【請求項20】 請求項18の前記情報配布装置と、請

求項19の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項21】 前記所定の情報が、金額情報または暗号鍵K_wであることを特徴とする請求項3、6、9、13、又は20のいずれかに記載の情報配布システム。

【請求項22】 所定の情報が金額情報であって、前記暗号化された金額情報を秘密鍵K_sで復号して前記金額情報を得た後、前記暗号化された金額情報を消去し、その消去が成功した場合のみ、前記得た金額情報を有効と判定することを特徴とする請求項21の情報配布システム。

【請求項23】 所定の情報が金額情報であって、前記暗号化された金額情報を秘密鍵K_sで復号して前記金額情報を得た後、その得た金額情報から使用分の金額を減額したときは、その減額後の金額情報を同一の暗号化方法により暗号化し、前記元の暗号化された金額情報を更新し、その更新が成功した場合のみ、前記減額を有効と判定することを特徴とする請求項21の情報配布システム。

【請求項24】 前記所定の情報は、少なくとも暗号鍵K_wを含み、前記情報記録媒体には前記暗号鍵K_wにより暗号化されたデータが記録されているものであって、前記判定手段により前記所定の情報が適正と判定された場合に、前記暗号鍵K_wで暗号化されたデータを復号するデータ復号手段を備えたことを特徴とする請求項2、5、8、又は12のいずれかに記載の端末装置。

【請求項25】 前記暗号化されたデータは、複数のデータに分割されていることを特徴とする請求項24記載の端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、暗号化された映画等のコンテンツを記録した記録媒体を配布し、ユーザがそれを購入して利用する情報配布装置及び端末装置と情報配布システムに関するものである。

【0002】

【従来の技術】 近年、映画や映像などの情報をCD-ROM、あるいはDVD-RAMなどの記録媒体に記録し、それをユーザに販売する方法が提案されている。このとき、情報の不正コピーによる使用や無断使用を防止するため、記録する情報を暗号化して、この暗号を解く鍵が無ければ映画や映像を見れないようにし、料金を支払った者のみこの暗号を解く鍵を入手して記録された情報を利用できるようにしている。従って、記録媒体に記録された暗号化情報は、不正コピーしたり、無断使用しようとしても、暗号を解く鍵を何らかの方法で入手しない限りは使用できない。

【0003】

【発明が解決しようとする課題】 しかしながら、このような方法では、暗号を解く鍵も暗号化情報が記録された

記録媒体と同様に、配布者側からユーザ側に伝達する必要があるため、盗まれたり、鍵そのものの不正コピーが発生する恐れがあり、その場合には、不正コピーによる使用や無断使用を防止できないという課題がある。

【0004】本発明は、従来のこのような課題を考慮し、他の記録媒体への不正コピーや無断使用を確実に防止できる情報配布装置及び端末装置と情報配布システムを提供することを目的とするものである。

【0005】

【課題を解決するための手段】請求項1の本発明は、記録媒体固有のID番号を持ち公開鍵Kpが記録された情報記録媒体から、ID番号及び公開鍵Kpを読み取る鍵読取り手段と、その読み取ったID番号及び所定の情報を読み取った公開鍵Kpにより暗号化する暗号化手段と、その暗号化したID番号及び所定の情報を情報記録媒体に記録する記録手段とを備えた情報配布装置である。

【0006】請求項2の本発明は、請求項1の情報配布装置で、公開鍵Kpにより暗号化したID番号及び所定の情報が記録された情報記録媒体から、ID番号、暗号化ID番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、公開鍵Kpに対応する秘密鍵Ksを用いて、読み取った暗号化ID番号及び所定の情報を復号する復号化手段と、その復号ID番号と前記ID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、復号した所定の情報を適正であると判定する判定手段とを備えた端末装置である。

【0007】請求項4の本発明は、記録媒体固有のID番号を持つ情報記録媒体から、ID番号を読み取るID読取り手段と、公開鍵Kpが記録された鍵記録媒体から公開鍵Kpを読み取る鍵読取り手段と、その読み取った公開鍵Kpにより読み取ったID番号及び所定の情報を暗号化する暗号化手段と、その暗号化したID番号及び、所定の情報を情報記録媒体に記録する記録手段とを備えた情報配布装置である。

【0008】請求項5の本発明は、請求項4の情報配布装置で、公開鍵Kpにより暗号化したID番号及び所定の情報が記録された情報記録媒体から、ID番号、暗号化ID番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、公開鍵Kpに対応する秘密鍵Ksを用いて、読み取った暗号化ID番号及び所定の情報を復号する鍵復号化手段と、その復号ID番号とID番号とを比較するID比較手段と、その比較の結果、ID番号が一致した場合に、復号した所定の情報を適正であると判定する判定手段とを備えた端末装置である。

【0009】

【発明の実施の形態】以下に、本発明をその実施の形態を示す図面に基づいて説明する。

（第1の実施の形態）図1は、本発明にかかる第1の実施の形態の情報配布装置及び端末装置の機能を説明する

構成図である。図1において、例えばDVD-RAM103を記録媒体として用い、このDVD-RAM103に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置101と、ユーザが購入したDVD-RAM103に記録された配布情報を再生する端末装置102により情報配布システムが構成されている。

【0010】ここで、端末装置102は、公開鍵暗号方式の解読鍵となる秘密鍵Ksが読み取り不可能な状態で内蔵され、DVD-RAM103には、記録媒体固有の一意に決まるID番号及び秘密鍵Ksと対になる暗号化のための公開鍵Kpが記録されている。ここでKs及びKpは端末に固有である。また、配布情報は通常の暗号鍵Kwにより暗号化され、予め記録されていてもよいし、配布時に記録するようにしてもよい。

【0011】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【0012】ユーザ配布情報を配布する場合、まず、配布装置101において、DVD-RAM103のID番号及び公開鍵Kpを読み取り、公開鍵KpによりID番号及び暗号鍵Kwが暗号化される。この暗号化されたものを便宜上Kp[ID, Kw]で表す。ここでは、配布装置101が暗号鍵KwとID番号との変換テーブルを持ち、暗号鍵Kwは読み取ったID番号に基づいて生成されるものとする。配布情報が予め記録されている場合、変換テーブルはID番号から、予め記録された情報を暗号化した暗号鍵Kwを特定するための変換作用を持つものとする。次に、暗号化されたKp[ID, Kw]が、DVD-RAM103に記録される。配布情報を暗号鍵Kwで暗号化したKw[DATA]もDVD-RAM103に記録されている。

【0013】次に、ユーザはこの状態のDVD-RAM103を購入し、所有する端末装置102を用いてDVD-RAM103を再生する。端末装置102において、まず、購入したDVD-RAM103からID番号及びKp[ID, Kw]を読み取り、その読み取ったKp[ID, Kw]を内蔵する秘密鍵Ksにより復号する。次に、復号したIDとDVD-RAM103から直接読み取ったIDとを比較し、比較結果が一致した場合に、復号した暗号鍵Kwを用いてDVD-RAM103から読み取ったKw[DATA]を復号し、図示しないAVデコーダを通じて、TVにより鑑賞する。

【0014】この時、比較結果が一致しない場合は、ID番号が各記録媒体に固有であることから、情報が他のDVD-RAMにコピーされていると判断できるので、暗号鍵Kwによる復号は停止される。

【0015】また、Kwによる配布情報の暗号化は共通鍵暗号方式により行うことが好適な構成である。これにより、復号に大きな計算量が必要な公開鍵の解読をKw

を入手する際のみとし、映画などの大量の情報を容易に復号できる。

〔第2の実施の形態〕図2は、本発明にかかる第2の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。図2において、例えばDVD-RAM203を情報記録媒体として用い、このDVD-RAM203に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置201と、ユーザが購入したDVD-RAM203に記録された配布情報Kw

[DATA]を再生する端末装置202により情報配布システムが構成されている。本実施の形態では、前述の第1の実施の形態と異なり、公開鍵KpをDVD-RAM203ではなく、ユーザが端末装置202を用いて、例えばICカード204等を用いた記録媒体（以後、鍵記録媒体と呼ぶ）に記録して配布装置201に提供する方法をとる。

〔0016〕ここで、端末装置202は、公開鍵暗号方式の解読鍵となる秘密鍵Ksが読み取り不可能な状態で内蔵され、DVD-RAM203には、記録媒体固有の一意に決まるID番号が記録されている。また、前述と同様、配布情報は通常の暗号鍵Kwにより暗号化され、予め記録されていてもよいし、配布時に記録するようにしてもよい。

〔0017〕図3は、本実施の形態の配布装置及び端末装置の内部を示すブロック図である。配布装置201は、ICカード204に記録された情報を読み取る鍵読取り手段としてのカード読取り手段211、DVDドライブ216で駆動されるDVD-RAM203から情報を読み取るID読取り手段としての読取り手段213、DVD-RAM203に情報を記録する記録手段215、ID番号を暗号鍵Kwに変換するKw・IDテーブル214、情報を暗号化する暗号化手段212により構成されている。

〔0018〕一方、端末装置202は、ICカード204に情報を記録するカード記録手段221、公開鍵Kp及びそれと対になる秘密鍵Ksを格納するメモリ226、DVDドライブ222で駆動されるDVD-RAM203から情報を読み取り分離する読取り分離手段223、暗号化情報を解読する2つの解読器225、227、2つの情報を比較する比較手段（例えば、マイコンで構成される）224により構成されている。ここで、読取り分離手段223が暗号読取り手段を構成し、解読器225が鍵復号化手段を構成し、比較手段224がID比較手段及び判定手段を構成している。

〔0019〕また、DVD-RAM203は、ROMエリアとRAMエリアで構成されており、配布装置201で記録するKp[ID, Kw]はRAMエリアに記録される。また、暗号化された配布情報Kw[DATA]はROMエリア、あるいはRAMエリアのどちらに記録されていてもよいが、ROMエリアの場合は予め記録して

おく。

〔0020〕次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

〔0021〕ユーザ配布情報を配布する場合、まず、端末装置202において、カード記録手段221がメモリ226から公開鍵Kpを読み出し、ICカード204に記録する。次に、配布装置201において、その公開鍵Kpが記録されたICカード204からカード読取り手段211が公開鍵Kpを読み取り、また、DVDドライブ216にセットされたDVD-RAM203から読取り手段213が、そのDVD-RAM203のID番号を読み取る。

〔0022〕カード読取り手段211により読み取られた公開鍵Kpは暗号化手段212に送られ、読取り手段213で読み取られたID番号は、Kw・IDテーブル214及び暗号化手段212に送られる。Kw・IDテーブル214では、ID番号に基づいて配布情報を暗号化するための暗号鍵Kwを生成し、生成した暗号鍵Kwを暗号化手段212に送る。次に、暗号化手段212は、ID番号及び暗号鍵Kwを公開鍵Kpにより暗号化し、この暗号化したKp[ID, Kw]を記録手段215に送る。記録手段215は、この暗号化されたKp[ID, Kw]をDVDドライブを介してDVD-RAM203のRAMエリアに記録する。この時、前述したように、配布情報を暗号鍵Kwで暗号化したKw[DATA]もDVD-RAM203に記録されている。

〔0023〕次に、ユーザはこの状態のDVD-RAM203を、所有する端末装置202を用いてDVD-RAM203を再生する。端末装置202において、まず、読取り分離手段223は、DVDドライブ222を介して、購入したDVD-RAM203からID番号及びKp[ID, Kw]を読み取り、それら情報を分離する。このとき、Kw[DATA]も読み取られて分離される。分離されたID番号は比較手段224に、Kp[ID, Kw]は解読器225に、Kw[DATA]は解読器227に、それぞれ送られる。

〔0024〕解読器225はメモリ226から公開鍵Kpと対になる秘密鍵Ksを読み出し、その秘密鍵Ksにより暗号化情報Kp[ID, Kw]を解読してID番号を比較手段224に送り、暗号鍵Kwを解読器227に送る。比較手段224では、読取り分離手段223からのID番号と解読器225で解読されたID番号とが比較され、比較結果に応じてON/OFF信号を解読器227に送る。すなわち、2つのID番号が一致すればON信号を出力し、一致しなければOFF信号を出力する。

〔0025〕解読器227は、ON信号のとき解読器225からの暗号鍵Kwによって、暗号化配布情報Kw[DATA]を解読して映画等のAVデータを出力す

る。AVデータは図示しないAVデコーダを通じて、TVにより鑑賞する。

【0026】前述の第1の実施の形態の場合と同様に、ID番号の比較結果が一致しない場合は、ID番号が各記録媒体に固有であることから、情報が他のDVD-RAMにコピーされていると判断できるので、暗号鍵Kwによる復号は停止される。

【0027】このように、本発明によれば、DVD-RAMのオリジナルとコピーとを判定することができる。この判定を逃れることを困難とするためには、IDを市販の機器によってはコピーできない領域（例えばROMか1回のみ書き込み可能な領域など）に記録しておくことが好適である。

【0028】ここで、第3者が上記で説明した端末（以下では適正な端末と呼ぶ）によらず、上記で説明した情報記録媒体のオリジナルではなくそのコピーにより情報を取得しようとした場合を説明する。

【0029】例えばDVD-RAMの固有のIDごと全てコピーが可能な装置を用いた場合、このようにして作ったコピーを、保持するKsが異なる他の端末で再生しようとすると、IDやKwを正しく復号化することができないため、情報を得ることができない。

【0030】また一方、特定の端末のKsが不正に暴露されるなどにより、他の端末に同一のKsを与えることが可能となった場合でも、本発明のコピー判定機能が働いている限りコピーにより生成された情報配布媒体から情報を得ることはできない。

【0031】以上のように、本発明の配布方法は、配布媒体のコピー防止とユーザ端末の特定機能を同時に備えているため、第3者が不正コピーや、無断で他の端末で利用することによって情報を不正取得することは著しく困難となり、不正に不特定多数の端末に情報のコピーを配布する行為を防止する効果がある。

（第3の実施の形態）図4は、本発明にかかる第3の実施の形態の情報配布装置及び端末装置を示すブロック図である。本実施の形態に用いるDVD-RAMは図5に示すような記録形態であり、配布情報が複数に分割され、その分割された部分情報がそれぞれ異なる暗号鍵K1～K4で暗号化され、更に、各暗号鍵K1～K4が暗号鍵Kwにより暗号化されている。すなわち、二重に暗号化されている。また、記録されている配布情報に対応して、それぞれの識別情報としてのタイトル名が記録されている。

【0032】図4において、図5のDVD-RAM303を情報記録媒体として用い、このDVD-RAM303に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置301と、ユーザが購入したDVD-RAM303に記録された配布情報を再生する端末装置302により情報配布システムが構成されている。本実施の形態では、鍵記録媒体としてのICカー

ド304に固有のID番号を利用し、公開鍵KpをICカード304に記録して配布装置301に提供し、暗号化情報をICカード304に記録する方法をとる。このICカード304は、ID番号が予め記録されているROMエリアと情報を記録可能なRAMエリアとを持つ。

【0033】配布装置301は、ICカード304に記録された情報を読み取る鍵読取り手段としてのカード読取り手段311、DVDドライブ316で駆動されるDVD-RAM303から情報（タイトル名）を読み取る識別情報読取り手段としての読取り手段313、ICカード304に情報を記録する情報記録手段としてのカード記録手段315、タイトル名を暗号鍵Kwに変換する情報生成手段としてのKw・タイトルテーブル314、情報を暗号化する暗号化手段312により構成されている。

【0034】一方、端末装置302は、ICカード304に情報を記録するカード記録手段321、公開鍵Kp及びそれと対になる秘密鍵Ksを格納するメモリ326、DVDドライブ322で駆動されるDVD-RAM303から情報を読み取り分離する読取り分離手段323、暗号化情報を解読する3つの解読器325、327、328、2つの情報を比較するID比較手段としての比較手段（例えば、マイコンで構成される）324、ICカード304の情報を読み取る暗号読取り手段としてのカード読取り手段329、タイトル名に基づいて配布情報を選択する選択手段330により構成されている。ここで、解読器325が復号化手段を構成している。

【0035】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【0036】ユーザが配布情報を購入する場合、まず、端末装置302において、カード記録手段321がメモリ326から公開鍵Kpを読み出し、ID番号が記録されたICカード304に記録する。次に、配布装置301において、その公開鍵Kpが記録されたICカード304からカード読取り手段311がID番号及び公開鍵Kpを読み取り、また、DVDドライブ316にセットされたDVD-RAM303から読取り手段313が、配布情報のタイトル名を読み取る。

【0037】カード読取り手段311により読み取られたID番号及び公開鍵Kpは暗号化手段312に送られ、読取り手段313で読み取られたタイトル名は、Kw・タイトル名テーブル314及びカード記録手段315に送られる。Kw・タイトル名テーブル314では、タイトル名に基づいて配布情報を暗号化するための暗号鍵Kwを生成し、生成した暗号鍵Kwを暗号化手段312に送る。次に、暗号化手段312は、ID番号及び暗号鍵Kwを公開鍵Kpにより暗号化し、この暗号化したKp[ID, Kw]をカード記録手段315に送る。カ

ード記録手段315は、この暗号化されたKp[ID, Kw]及び暗号化されていないタイトル名をICカード304のRAMエリアに記録する。この時、前述したように、配布情報は4分割されて、暗号鍵K1~K4によりそれぞれ暗号化されており、それら暗号鍵K1~K4も暗号鍵Kwで暗号化されている。配布情報の分割数は4に限定されるものではなく、暗号鍵の個数も分割数に応じて用意すればよい。尚、図5では、暗号化した配布情報をK1[DATA]~K4[DATA]で表している。

【0038】次に、ユーザはこの状態のDVD-RAM303を購入し、所有する端末装置302により、ICカードに記録された情報を利用してDVD-RAM303を再生する。端末装置302において、まず、カード読取り手段329は、ICカード304に記録されたID番号、暗号化情報Kp[ID, Kw]、タイトル名を読み取り、選択手段330に送る。

【0039】一方、読取り分離手段323は、DVDドライブ322を介して、購入したDVD-RAM303からタイトル名、Kw[K1]~Kw[K4]、K1[DATA]~K4[DATA]を読み取り、それら情報を分離する。分離されたタイトル名は選択手段330に、Kw[K1]~Kw[K4]は解読器328に、K1[DATA]~K4[DATA]は解読器327に、それぞれ送られる。選択手段330は、ID番号を比較手段324に送るとともに、読取り分離手段323からのタイトル名に応じて、そのタイトル名に対応する暗号化情報Kp[ID, Kw]を選択し、そのKp[ID, Kw]を解読器325に送る。

【0040】解読器325はメモリ326から公開鍵Kpと対になる秘密鍵Ksを読み出し、その秘密鍵Ksにより暗号化情報Kp[ID, Kw]を解読してID番号を比較手段324に送り、暗号鍵Kwを解読器328に送る。解読器328は暗号鍵Kwを用いて暗号情報Kw[K1]~Kw[K4]を解読して暗号鍵K1~K4を解読器327に出力する。

【0041】また、比較手段324は、選択手段330からのID番号と解読器325で解読されたID番号とを比較し、比較結果に応じてON/OFF信号を解読器327に送る。すなわち、2つのID番号が一致すればON信号を出力し、一致しなければOFF信号を出力する。

【0042】解読器327は、ON信号のとき解読器328からの暗号鍵K1~K4によって、暗号化配布情報K1[DATA]~K4[DATA]をそれぞれ解読してAVデータを出力する。AVデータは図示しないAVデコードを通じて、TVにより鑑賞する。

【0043】前述の第1の実施の形態の場合と同様に、ID番号の比較結果が一致しない場合は、暗号鍵Kwによる復号は停止されるとともに、暗号鍵Kw、ID番号

がDVD-RAMと別の記録媒体で運ばれるため、より安全性が増し、更に、配布情報を暗号化する暗号鍵を二重にしているため、不正コピー、無断利用に対して更に安全度が高くなる。

(第4の実施の形態)図6は、本発明にかかる第4の実施の形態の情報配布装置及び端末装置を示すブロック図である。本実施の形態に用いるDVD-RAMは図7に示すような記録形態であり、前述の図5と同様に、配布情報が複数に分割され、その分割された部分情報がそれぞれ異なる暗号鍵K1~K4で暗号化され、更に、各暗号鍵K1~K4が暗号鍵Kwにより暗号化されている。図5の場合と異なる点は、タイトル名は記録せず、ROMエリアが設けられ、そのROMエリアにDVD-RAMに固有のID番号が記録されている点である。

【0044】図6において、図7のDVD-RAM403を情報記録媒体として用い、このDVD-RAM403に映画などの情報(以後、配布情報と呼ぶ)を記録してユーザに配布する配布装置401と、ユーザが購入したDVD-RAM403に記録された配布情報を再生する端末装置402により情報配布システムが構成されている。本実施の形態では、前述の第2の実施の形態と同様に、公開鍵Kpをユーザが端末装置402を用いて、鍵記録媒体としてのICカード404に記録して配布装置401に提供し、暗号化された情報をDVD-RAM403に記録する方法をとる。

【0045】配布装置401は、ICカード404に記録された情報を読み取る鍵読取り手段としてのカード読取り手段411、DVDドライブ416で駆動されるDVD-RAM403から情報を読み取るID読取り手段としての読取り手段413、DVD-RAM403に情報を記録する記録手段415、ID番号を暗号鍵Kwに変換する情報生成手段としてのKw・IDテーブル414、情報を暗号化する暗号化手段412により構成されている。

【0046】一方、端末装置402は、ICカード404に情報を記録するカード記録手段421、公開鍵Kp及びそれと対になる秘密鍵Ksを格納するメモリ426、DVDドライブ422で駆動されるDVD-RAM403から情報を読み取り分離する暗号鍵読取り手段としての読取り分離手段423、暗号化情報を解読する3つの解読器425、427、428、2つの情報を比較するID比較手段としての比較手段(例えば、マイコンで構成される)424により構成されている。ここで、解読器425が鍵復号化手段を構成し、解読器428が暗号鍵復号手段を構成し、解読器427がデータ復号手段を構成している。

【0047】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【0048】ユーザが配布情報を購入する場合、まず、

端末装置402において、カード記録手段421がメモリ426から公開鍵Kpを読み出し、ICカード404に記録する。次に、配布装置401において、その公開鍵Kpが記録されたICカード404からカード読取り手段411が公開鍵Kpを読み取り、また、DVDドライブ416にセットされたDVD-RAM403から読取り手段413が、そのDVD-RAM403のID番号を読み取る。

【0049】カード読取り手段411により読み取られた公開鍵Kpは暗号化手段412に送られ、読取り手段413で読み取られたID番号は、Kw・IDテーブル414及び暗号化手段412に送られる。Kw・IDテーブル414では、ID番号に基づいて配布情報を暗号化するための暗号鍵Kwを生成し、生成した暗号鍵Kwを暗号化手段412に送る。次に、暗号化手段412は、ID番号及び暗号鍵Kwを公開鍵Kpにより暗号化し、この暗号化したKp[ID, Kw]を記録手段415に送る。記録手段415は、この暗号化されたKp[ID, Kw]をDVDドライブを介してDVD-RAM403のRAMエリアに記録する。この時、前述したように、配布情報は4分割されて、暗号鍵K1~K4によりそれぞれ暗号化されており、それら暗号鍵K1~K4も暗号鍵Kwで暗号化されている。配布情報の分割数は4に限定されるものではなく、暗号鍵の個数も分割数に応じて用意すればよい。

【0050】次に、ユーザはこの状態のDVD-RAM403を購入し、所有する端末装置402を用いてDVD-RAM403を再生する。端末装置402において、まず、読取り分離手段423は、DVDドライブ422を介して、購入したDVD-RAM403からID番号、暗号情報Kp[ID, Kw]、Kw[K1]~Kw[K4]、K1[DATA]~K4[DATA]を読み取り、それら情報を分離する。分離されたID番号は比較手段424に、Kp[ID, Kw]は解読器425に、Kw[K1]~Kw[K4]は解読器428に、K1[DATA]~K4[DATA]は解読器427に、それぞれ送られる。

【0051】解読器425はメモリ426から公開鍵Kpと対になる秘密鍵Ksを読み出し、その秘密鍵Ksにより暗号化情報Kp[ID, Kw]を解読してID番号を比較手段424に送り、暗号鍵Kwを解読器428に送る。解読器428は暗号鍵Kwを用いて暗号情報Kw[K1]~Kw[K4]を解読して暗号鍵K1~K4を解読器427に出力する。

【0052】また、比較手段424は、読取り分離手段423からのID番号と解読器425で解読されたID番号とを比較し、比較結果に応じてON/OFF信号を解読器427に送る。すなわち、2つのID番号が一致すればON信号を出力し、一致しなければOFF信号を出力する。

【0053】解読器427は、ON信号のとき解読器428からの暗号鍵K1~K4によって、暗号化配布情報K1[DATA]~K4[DATA]をそれぞれ解読してAVデータを出力する。AVデータは図示しないAVデコーダを通じて、TVにより鑑賞する。

【0054】前述の第1の実施の形態の場合と同様に、ID番号の比較結果が一致しない場合は、暗号鍵Kwによる復号は停止されるとともに、更に、配布情報を暗号化する暗号鍵を二重にしているので、不正コピー、無断利用に対して更に安全度が高くなる。

(第5の実施の形態) 図8は、本発明にかかる第5の実施の形態における記録媒体上の記録状態を示す図である。本実施の形態は、基本的には例えば、第2の実施の形態などと同じであるが、公開鍵Kpにより暗号化されたID番号及び暗号鍵Kwである暗号化情報Kp[ID, Kw]を、元の鍵記録媒体であるICカードや情報記録媒体であるDVD-RAM503のRAMエリアに記録する代わりに、別の鍵記録媒体、例えば図8に示すように、DVD-RAM503の所定領域に設けられた鍵媒体(例えば、バーコード形式などによるもの)に記録するものである。尚、この別の鍵記録媒体はDVD-RAM503上に設けることは、特に限定されるものではない。

(第6の実施の形態) 図9は、本発明にかかる第6の実施の形態における記録媒体上の記録状態を示す図である。本実施の形態は、例えば第2の実施の形態において、ID番号の代わりにDVD-RAM(情報記録媒体)603に固有の一意的に決まっている暗号鍵KIDをROMエリアに持たせて、これを利用するものであり、配布情報を暗号化するための暗号鍵Kwを暗号鍵KIDにより暗号化し、この暗号化したKID[Kw]を更に公開鍵Kpによって暗号化して、その暗号化情報Kp[KID[Kw]]をRAMエリアに記録するものである。この方法によれば、暗号鍵KIDがDVD-RAMに固有であるため、別のDVD-RAMにコピーされても、読み取った暗号鍵KIDが異なるため、仮に公開鍵Kpと対になる秘密鍵Ksを盗まれても暗号鍵Kwを復号出来ず、不正利用が防止できる。

【0055】例えば、第1の実施の形態では、Ksが暴露され、かつ端末のコピー判定機能が解除された場合、固有のIDごと情報記録媒体のコピーができなくとも、他の端末でコピーの再生が行える可能性が残った。しかし、記録媒体に固有の鍵KIDを使う方式においては、更に、KIDごと情報記録媒体のコピーが行われた場合にだけ不正に再生が可能であり、より安全性が高くなる。

【0056】なお、上記実施の形態では、いずれも公開鍵Kpにより暗号化する所定の情報として暗号鍵としたが、これに限らず、例えば支払った金額の料金情報(課金情報)などであってもよい。あるいは又、それら両者を含んでいてもよい。料金情報を用いれば、支払った金

額分の情報のみ復号することにより、1枚の情報記録媒体に多種類の情報を記録して販売しても、ユーザが利用できる情報や利用回数を制限できる。上記の料金情報を用いる場合は、例えば、端末装置において、暗号化された料金情報を読み取って復号した後、その暗号化された料金情報を消去する。この消去が成功した場合に限り、復号した料金情報を有効とする。このようにすれば、料金情報が何度も再利用されることがなく、不正使用が防止できる。また、金額分の一部だけ情報を利用したときは、料金情報を更新する必要がある。この場合は、元の料金情報から使用金額分を減額した後、同じ暗号化方法で暗号化し、その暗号化した料金情報を元の暗号化情報に上書きし、その上書きが成功した場合に限り料金情報を有効とする。

【0057】また、上記第3の実施の形態では、識別情報としてタイトル名を用いたが、これに限らず、識別情報は記録するデータのコンテンツを識別できるものであればよく、例えば、タイトルIDなどでもよい。

【0058】また、上記実施の形態では、いずれも情報記録媒体としてDVD-RAMを例に説明したが、これに限らず、例えば、CD-ROMやCD-R等であってもよい。

【0059】また、上記実施の形態では、いずれも鍵記録媒体としてICカードを例に説明したが、これに限らず、例えば、磁気カード等であってもよい。

【0060】

【発明の効果】以上述べたところから明らかなように本発明は、記録媒体固有のID番号及び所定の情報を公開鍵暗号方式により暗号化し、その暗号化したID番号を復号したID番号と記録媒体から読み取ったID番号とを比較することにより、所定の情報が適正かどうかを判定しているので、他の記録媒体への不正コピーや無断使用を確実に防止できるという長所を有する。

【図面の簡単な説明】

【図1】本発明にかかる第1の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。

【図2】本発明にかかる第2の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。

【図3】同第2の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図4】本発明にかかる第3の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図5】同第3の実施の形態における記録媒体上の記録状態を示す図である。

【図6】本発明にかかる第4の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図7】同第4の実施の形態における記録媒体上の記録状態を示す図である。

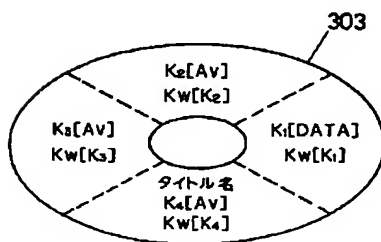
【図8】本発明にかかる第5の実施の形態における記録媒体上の記録状態を示す図である。

【図9】本発明にかかる第6の実施の形態における記録媒体上の記録状態を示す図である。

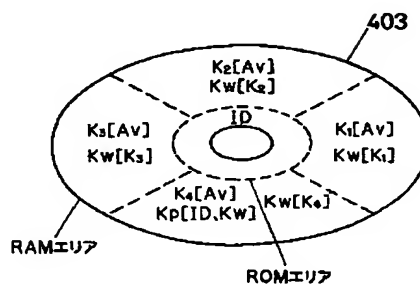
【符号の説明】

101、201、301、401	配布装置
102、202、302、402	端末装置
103、203、303、403、503、603	DVD-RAM
204、304、404	ICカード
212、312、412	暗号化手段
215、415	記録手段
223、323、423	読取り分離手段
224、324、424	比較手段
225、325、425	解読器
227、327、427	解読器
328、428	解読器

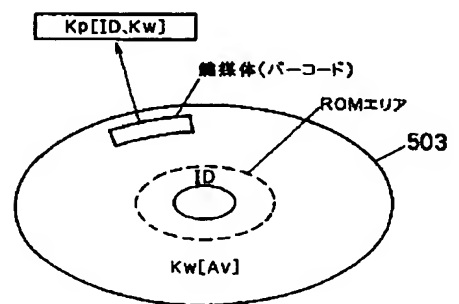
【図5】



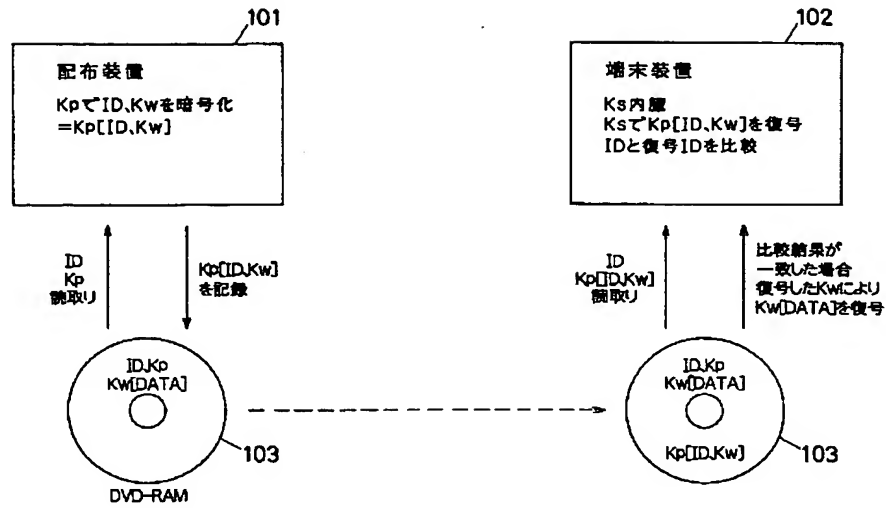
【図7】



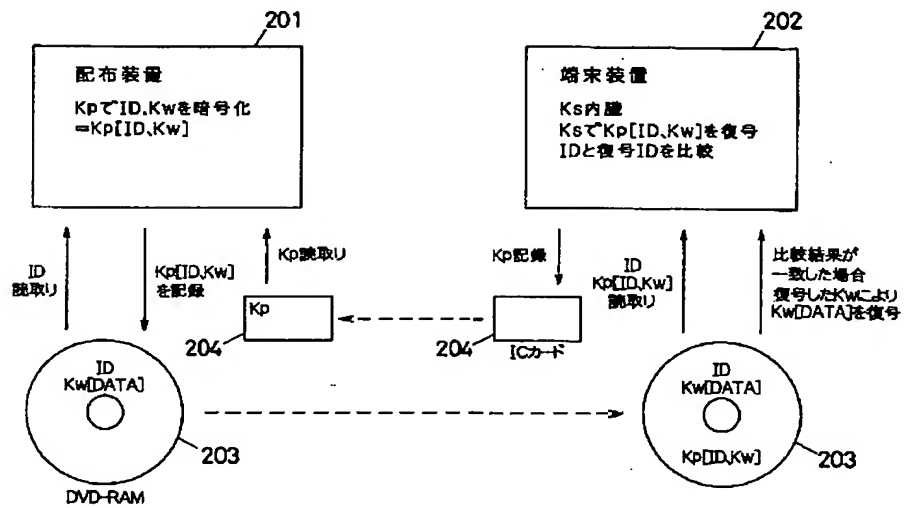
【図8】



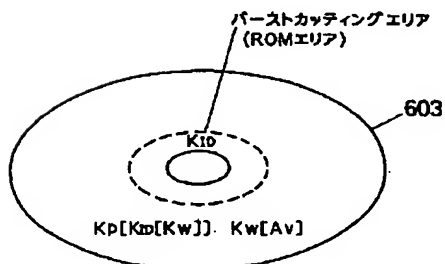
【図1】



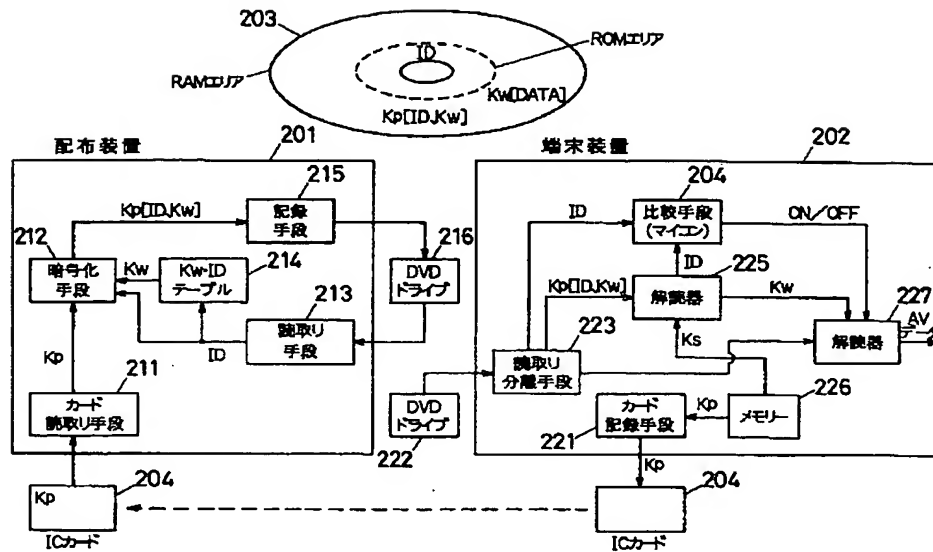
【図2】



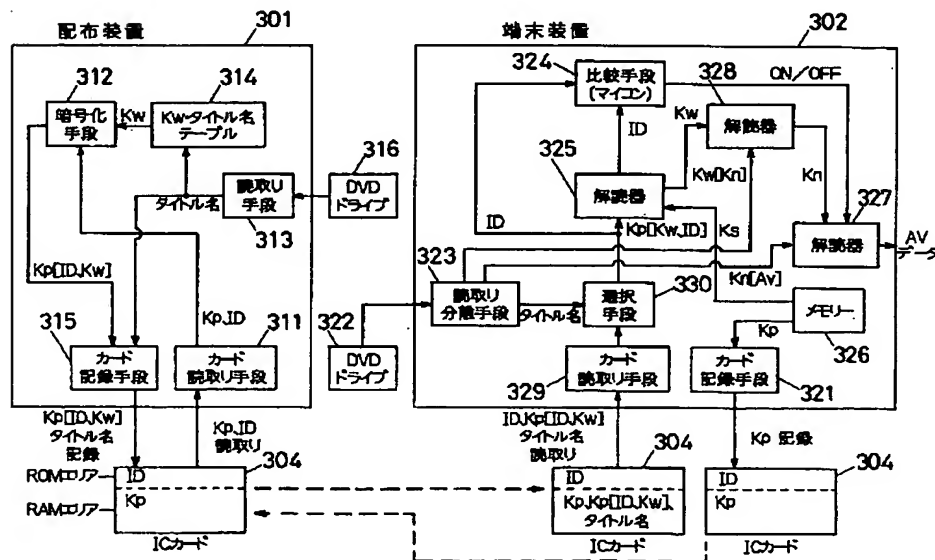
【図9】



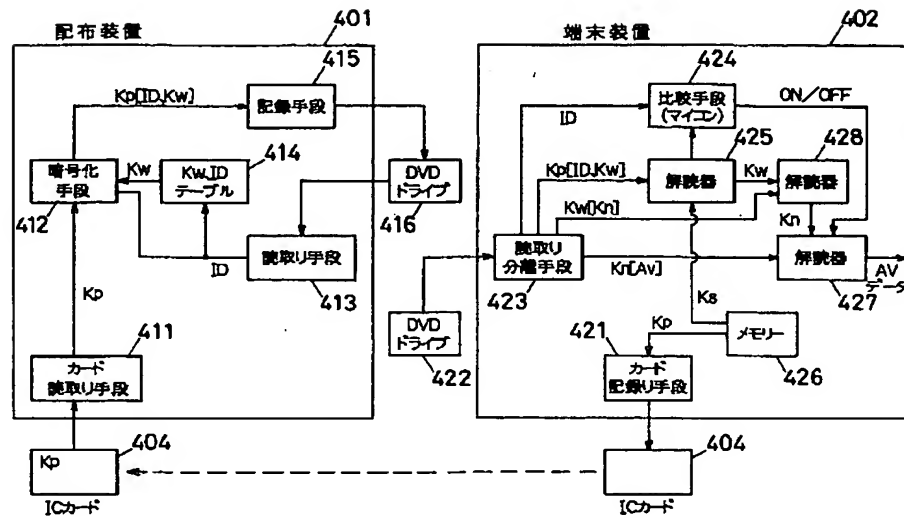
【図3】



【図4】



【図6】



フロントページの続き

(72)発明者 山田 正純
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内